MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

13 March 2019

Ref: DOIA 1819-1013

[redacted]

Dear [redacted]

Thank you for your email of 9 January 2019 to the Ministry of Business, Innovation and Employment requesting, under the Official Information Act 1982 (the Act), the following information:

> *copies of all training material provided by ZX Security for the "advanced social media training course" delivered above. The contract explicitly refers to powerpoint presentations, so those and any course notes would be a good place to start.*

Your request is refused under section 6(c) of the Act, as the making available of the information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial. The information requested is also withheld under section 9(2)(b)(ii) of the Act, as the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information. I do not consider that the withholding of this information is outweighed by public interest considerations in making the information available.

However, please find attached a copy of the document *Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory, compliance and enforcement work* which applies to all MBIE employees. Please note these procedures are currently being reviewed. Some information in this document has been withheld under the following sections of the Act:

- section 6(c), as the the making available of that information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial; and
- section 9(2)(g)(ii), to maintain the effective conduct of public affairs through the protection of such Ministers, members of organisations, officers, and employees from improper pressure or harassment. I do not consider that the withholding of this information is outweighed by public interest considerations in making the information available.

MBIE has procedures and guidelines in place in relation to the use of social media for both verification and investigation purposes. These procedures help ensure the use of social media for verification and investigation purposes is being carried out in a safe and appropriate manner. They are supported by staff training provided by ZX Security as well as by internal processes.

MBIE is a regulator and therefore has the responsibility to ensure that regulations are complied with and enforced, and we need to be assured of the information we receive and on which decisions are taken.

As per the Master Agreement for advanced social media search training with ZX Security, a number of optional modules have been offered to MBIE, including topics such as methods for automated harvesting,

image metadata analysis and creating a dossier. To date, no MBIE staff have participated in these optional modules.

As a result of the State Services Commission's external security consultants' inquiry findings, MBIE is reviewing its current arrangements and taking a number of additional steps to ensure we are responding fully to the inquiry's recommendations. This includes appointing a senior leader to check we have the systems and processes in place to adhere to the new model standards for information gathering. ZX has not run the advanced social media training for MBIE staff since June 2018.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely

Adrian Regnault
General Manager
Enterprise, Risk and Assurance

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Procedures for MBIE staff using social media for verification and investigation purposes to support regulatory, compliance and enforcement work

January 2018

Version 1.0

New Zealand Government

Contents

Contents 2
Overview 3
Assess risk of using social media and determine access method 5
Confirm access option for using social media 7
Complete training for using social media 10
Obtain approval for using social media 10
Set up systems for using social media 12
Monitoring the use of social media 12
The Privacy Act and the use of social media 13
Official Information Act requests for details about social media 13
Appendix 1: Template for approval of overt passive membership for an individual or business unit 14
Appendix 2: Template for approval of discreet searching or discreet active engagement for an individual or business unit 15
Appendix 3: Process Overview 17
Appendix 4: Supporting documents 18

Overview

1. Purpose

The purpose of this document is to help manage the risks for MBIE staff who gather information through social media for regulatory, compliance and enforcement work by providing a process, procedures and guidelines that they can consistently use.

This process takes immediate effect and supersedes the Interim Advice provided to INZ and MSG General Managers by the Health, Safety and Security Implementation Programme Director, Shayne Gray, on 23 November 2016.

If you have any questions about this process, please contact the Manager Protective Security in the Corporate Governance and Information Group.

2. Scope

This procedure applies to all MBIE staff that use social media to assist their regulatory, compliance and enforcement work.

The procedures include:

1. Assess risk of using social media for work purposes
2. Determine access option for using social media
3. Complete training for using social media
4. Obtain approval for using social media
5. Set up systems for using social media.

Further guidance includes:

- Monitoring the use of social media
- How the requirements of the Privacy Act apply to the use of social media
- How to manage Official Information Act requests for details about social media.

3. Definition of terms

Term	Description
Discreet active engagement (false persona)	Accessing social media using an account with a false persona and actively engaging with individuals – this is not encouraged in MBIE.
Discreet searching (false persona)	Accessing social media using an account with a false persona and passively viewing information.
Entity	Any type of business, for example, a company, trust, sole trader or partnership.
False persona	A fictitious name or pseudonym used instead of a person's real name to conceal their identity.
Individual	A single, named person.
MBIE profile	A social media account set up with an individual's name with an MBIE owned suffix, e.g. firstname.lastname@mbie.govt.nz
Open (unregistered) searching	Accessing social media using a generic search engine where no registration is required.
Overt passive membership	Accessing social media by logging into a social media forum or community site using an MBIE account and passively observing individuals (e.g. Facebook).
Social media	The collective of online communication channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation and wikis are all examples of social media.
Stand-alone computer	Any laptop or desktop computer that can run local applications on its own without needing a connection to the MBIE network. Although it may be connected to a network, it is still a stand-alone computer as long as the network connection is not required for its general use.

Assess risk of using social media and determine access method

1. High-level risks

The use of social media for verification and investigation purposes in support of regulatory, compliance and enforcement work needs to be a considered decision. Information gathered from social media may or may not be valuable and, irrespectively, accessing the information carries risks that must be managed.

At a high level, the risks of using social media to gather information for verification and investigation purposes to support regulatory, compliance and enforcement work may be to:

- the rights of New Zealand's citizens and visitors
- the personal safety of staff or their family
- the security of MBIE's ICT network
- MBIE's reputation and legal liability
- the work of other agencies – domestically and internationally – should MBIE's activities inadvertently overlap with their activities.

2. Use of personal networks, devices and accounts are prohibited

Risks cannot be managed if staff use personal networks, personal devices or personal accounts for searching social media for verification or investigation purposes, therefore these methods are prohibited.

Staff are required to use MBIE's network, devices or accounts, or standalone systems, as agreed as part of the approvals process.

3. Methods of access

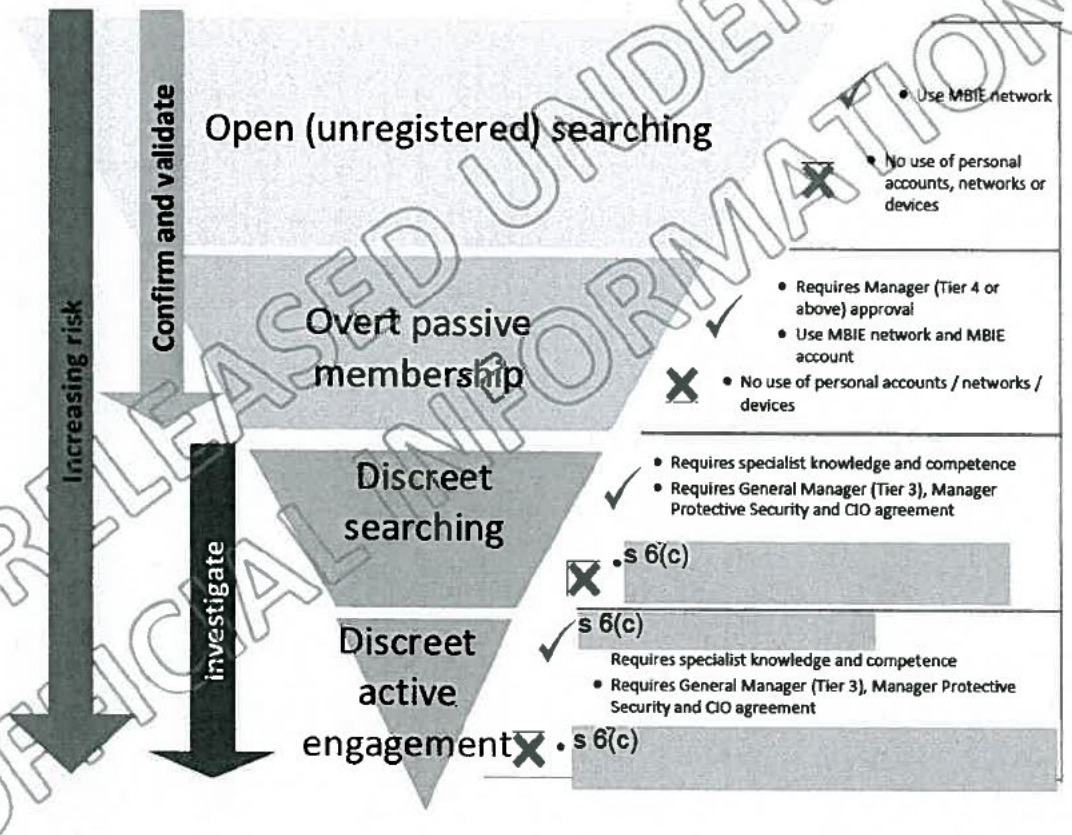
The risks associated with the use of social media vary depending on the method used to access the information. MBIE has identified four methods for accessing information from social media. In order of preferred use, with the most preferred and least risk first, they are:

Method	Purpose	What this looks like
Open (unregistered) searching -no account required -no approval required	To confirm or validate concerns using information that is publicly available and not subject to personalised privacy settings.	Accessing social media information using a generic search engine where no account registration or logging in is required (e.g. searching on a person's name using Google). Is undertaken using MBIE device and network.
Overt passive membership -use of @mbie.govt.nz account -approval required	To access and confirm or validate information that may be considered publicly available but is subject to personalised privacy settings that require an account login to view.	Accessing information via social media community membership that requires an account and to be logged in, using an MBIE-profile (@mbie.govt.nz), and only **passively** viewing information. This applies to social media communities like Facebook or LinkedIn and when logged in to search engines like Google Groups.

Discreet searching (false persona) -use of false persona account -approval required	To investigate a specific personal entity in relation to a specific task or case, when it would not be appropriate for the MBIE staff member's identity to be revealed.	s 6(c)
Discreet active engagement (false persona) -use of false persona account -approval required -systems required	To directly engage a specific personal entity in relation to a specific case, when it would not be appropriate for the MBIE staff member's identity to be revealed.	s 6(c)

The diagram below summarises the four access methods and how they are used.

Diagram 1: Accessing information



Confirm access option for using social media

1. Open (unregistered) searching

Description

MBIE's preferred search method is to use a generic search engine to gather information from social media on individuals or entities.[1] In practice, this means using the MBIE ICT network and then typing the name of the person or entity directly into Google (or another search engine) and observing only what is returned.

Social Search Engines are another option that allow you to view material without logging in to any specific social media platform, for example:

- s 6(c)
-

If you are gathering information via social media for the purpose of confirming or validating aspects of a case or decision to be made, this is the recommended approach to take.

Training

All staff using open (unregistered) searching must complete the Social Media for Verification and Investigation – Foundation training course available through Learn@MBIE.

Approval

Open (unregistered) searching for work purposes, does not require approval. Essentially this approach is a Google search. Staff do not need permission for non-login searching of the internet. Everyone searches Google and may find social media information, not subject to privacy settings, in this way.

2. Overt passive membership

This is similar to open (unregistered) searching, except that you are required to register and log in, increasing the risk level. This engagement method should only be used to verify and confirm information and does require management approval.

As soon as you encounter any information that may lead to a formal investigation, you must obtain the appropriate approvals and switch to discreet searching (false persona) or discreet active engagement (false persona).

When registering with the social media site, you must be clearly identified as part of MBIE and so must create and use an MBIE branded profile, i.e. *firstname.lastname@mbie.govt.nz*.

Training

All staff using overt passive membership must complete the Social Media for Verification and Investigation – Foundation training course available through Learn@MBIE.

[1] Depending on the privacy settings of the account holder, staff may be able to view all, some, or none of their social media information.

Approval

Overt passive membership for work purposes must be approved by your Manager (Tier 4 or above). The request and approval should be made by email, using the template at **Appendix 1**, and saved in your branch filing system for future reference.

Approving managers also have discretion to jointly grant permission to undertake overt passive membership either at an individual or at a business unit level and on a one off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

3. Discreet searching (false persona)

Discreet searching is used for verification or investigation into matters where grounds for further information gathering have been identified. The decision to transition from overt passive membership to discreet searching will be assessed on a case by case basis. Where there is a risk to the staff member or MBIE, should the identity of the staff member or the organisation performing the searching be revealed, it is recommended discreet searching using a false persona is used.

Discreet searching is:

- s 6(c)
- s 6(c)
- passive – you must not post, like, share, message or friend any of the individuals or entities you are viewing.

Even with passive use, be aware that if you log in to social media and view other people's accounts you may show up in an equivalent of a "Who's viewed your profile" panel (as happens with LinkedIn).

Discreet searching has risks to your personal safety as well as for the security of MBIE's ICT network. For these reasons, false personas used for discreet searching must be carefully established, maintained and replaced, as set out in the Social Media False Persona Guidelines. You will agree the most appropriate option for your work with the Chief Information Officer and Manager Protective Security as part of the approval process.

Training

Those staff that need to access social media using a false persona must complete both the Social Media for Verification and Investigation – Foundation course and the Social Media for Verification and Investigation – Advanced course, available through Learn@MBIE.

Approval

Discreet searching (false persona) for work purposes must be approved using the template at **Appendix 2**, and saved in your branch filing system for future reference.

Your General Manager (Tier 3) will approve any request to undertake discreet searching, confirming this is appropriate for the business.

The Chief Information Officer will approve the information management approach and the technology tool used to complete the task.

The Manager Protective Security will approve the approach from a security perspective.

Approving managers also have discretion to jointly grant permission to undertake discreet searching either at an individual or at a business unit level and on a one-off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

Where a request is urgent, that is, access to social media is required more quickly than the usual process allows, the request can be escalated to the respective branch Deputy Chief Executive to approve.

4. Discreet active engagement (false persona)

Discreet active engagement is where a social media account is used with a false persona to actively engage with an individual or entity. Discreet active engagement is a specialised area of expertise, requiring particular competence, and should only be used where there is appropriate cause to investigate using this method.

MBIE does not encourage active engagement using a false persona because the personal and reputational risks increase significantly. If you consider discreet active engagement is necessary, then your manager must consult with their General Manager (Tier 3), the Manager Protective Security and the Chief Information Officer to determine next steps.

You must set up a new social media account under a false persona for each investigation that requires discreet active engagement. A single social media account must not be used across more than one investigation, to avoid compromising either the account or the investigation, as set out in the Social Media False Persona Guidelines.

s 6(c) You will agree the most appropriate option for your work with the Chief Information Officer and Manager Protective Security as part of the approval process.

Training

Those staff that need to access social media using a false persona must complete both the Social Media for Verification and Investigation – Foundation course and the Social Media for Verification and Investigation – Advanced course, available through Learn@MBIE.

Approval

Discreet active engagement (false persona) for work purposes must be approved using the template at Appendix 2, and saved in your branch filing system for future reference.

Your General Manager (Tier 3) will approve any request to undertake discreet active engagement, confirming this is appropriate for the business.

The Chief Information Officer will approve the information management approach and the technology tool used to complete the task.

The Manager Protective Security will approve the approach from a security perspective.

Approving managers also have discretion to jointly grant permission to undertake discreet active engagement either at an individual or at a business unit level and on a one-off or ongoing basis. Where ongoing approval is granted, this must be reviewed and updated on an annual basis.

Where a request is urgent, that is, access to social media is required more quickly than the usual process allows, the request can be escalated to the respective branch Deputy Chief Executive to approve.

Complete training for using social media

1. Foundation course

All staff using social media must complete the Social Media for Verification and Investigation – Foundation course before requesting approval to access and use information from social media.

The Foundation course is available through Learn@MBIE.

2. Advanced course

Those staff that need to access social media using a false persona must also complete the Social Media for Verification and Investigation – Advanced course (or equivalent).

The Advanced course is available through Learn@MBIE.

Obtain approval for using social media

1. Approval form

All requests to access and use information from social media must be submitted using the appropriate template. See Appendices 1 and 2.

All approval forms must be saved in the branch filing system.

2. Individual or group approval

All staff using social media must gain appropriate approval for the access option they use. Approval to use social media for work purposes will usually be given on an individual, case-by-case basis.

Where the use of social media is a constant part of a business unit's work, approving managers will have discretion to grant ongoing permission to undertake information gathering via social media at a business unit level.

3. Approval for MBIE staff working overseas

MBIE staff working off-shore will follow the same approval processes as other staff, with additional approval steps from the Operations Manager, Risk Manager and Area Manager.

The Risk Manager is required to assess the social media request to determine if there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational or security factors.

The Risk Manager is responsible for obtaining local advice on the legality of the request. If legal advice has been provided previously for a similar request, then the Risk Manager can take that into account rather than obtaining additional local legal advice. The Risk Manager and their local legal advisor will consult with MBIE Legal New Zealand, where necessary, to clarify any legal risks or concerns.

4. Approvers' roles and responsibilities

The approval roles and responsibilities are summarised in the following table.

Role	Responsibilities
Chief Security Officer (CSO)	Approve the process and procedures for MBIE staff using social media for verification and investigation purposes to support regulatory, compliance and enforcement work.
Protective Security Requirements (PSR) Governance Committee	Review the process and procedures, and recommend changes and / or acceptance to the CSO.
Managers (Tier 4)	Approve requests to use overt passive membership of social media for verification and investigation purposes.
General Managers (Tier 3)	Responsible for health, safety and security of their staff. Approve requests to use discreet searching and discreet active engagement of social media for verification and investigation purposes.
Chief Information Officer(CIO)	Approve use of technology that provides a safe platform for discreet searching and discreet active engagement use of social media for verification and investigation purposes. Ensure information management is safe and appropriate.
Manager Protective Security	Approve that the approach to discreet searching and discreet active engagement use of social media, for verification and investigation purposes, is appropriately secure. Responsible for the maintenance of the process and procedures.
All Managers	Ensure all staff using social media for verification and investigation purposes have undertaken the appropriate training and complete the appropriate registers of use.
All Staff	Ensure the use of social media for verification and investigation purposes is undertaken in an appropriate manner.
Off-shore Risk, Operations and Area Manager	Approve requests for off-shore use of social media. Determines if there are any local factors that pose an additional risk to MBIE.
IRCB	Integrated Regulatory Compliance Branch responsible for the central register – a summary of the individual unit registers.
Deputy Chief Executive	Approves urgent social media requests where social media access is required more quickly than the normal process would allow.

5. Approval costs

Approving the request for use of social media confirms the business manager agrees to fund the necessary training, systems or equipment required to enable their staff to use social media in a safe and secure manner for work purposes.

An overview of the process for using social media for verification and investigation purposes is given in **Appendix 3.**

Set up systems for using social media

1. Establishment, maintenance and termination of false persona

The False Persona Guidelines must be used to set up, maintain and terminate false personas to be used for Discreet Searching (false persona) and discreet active engagement (false persona). Where a team is a high user of social media for verification and investigation purposes, it may be appropriate to set up and maintain a suite of false personas.

2. Register of accounts and use of social media

Each unit of a branch using social media must maintain a register of use, using the Social Media Usage Register template on the Critical Risk Management hub, and save it in their unit filing system. The register must be updated when social media is used for verification and investigation purposes in support of regulatory, compliance and enforcement work. If you wish to change the structure of the Usage Register, this must be agreed with the Integrated Regulatory Compliance Branch (IRCB).

Where a social media request is declined, the declined request and reason for the decline is to be logged in the decline table.

A central register will be maintained by the IRCB. A copy of the unit register must be sent to IRCB each month at socialmedia.registries@mbie.govt. The central register will provide a summary of the use of discreet searching (false persona) and discreet active engagement (false persona) and allow oversight of the use of social media within MBIE.

3. How to manage the collection and storage of evidence

The collection and storage of information will be managed as agreed in the approval process. This will usually involve taking screenshots and saving them into Word documents. These documents need to be saved within an appropriately secure filing structure. The information collected should be noted in the register.

4. Equipment required for use of social media

s 6(c) e of social media requires th s 6(c) You will agree the most appropriate option for your work with the Chief Information Officer and Manager Protective Security as part of the approvals process.

Monitoring the use of social media

As this is a new process, it is important to understand how staff respond to the changes in the use of social media, while ensuring the procedures are fit for purpose now and in the future as new social media platforms arise.

The use of social media across MBIE will be monitored by IRCB and the Protective Security Team, to gather information on the use, benefits, costs and issues of using social media as set out in these procedures. The monitoring will be used to refine the procedures and ensure staff are operating within the process to keep themselves safe online. Monitoring will include the:

- branch/units using social media

- use of social media access options
- use of social media sites
- value of the information gathered through social media for verification and investigation work, including number and type of cases
- number of staff completing social media training and the cost of it
- suitability and cost of equipment
- compliance by staff with the social media procedure.

The Privacy Act and the use of social media

Information posted on social media is subject to the Privacy Act 1993 if the information is about an individual. The main requirements are that:

- the collection of the information is necessary for a lawful purpose connected to the function of the agency
- information is collected lawfully and fairly and in a manner that does not unreasonably intrude on the individual
- information is accurate and where possible corroborated
- information is held and transferred safely and securely
- information is only used and shared for the reasons it has been collected.

Staff using overt passive membership, discreet searching and discreet active engagement methods to access and collect information through social media for verification and investigation purposes to support compliance, regulatory and enforcement work, must comply with the requirements of the Privacy Act 1993.

To evidence compliance with the Privacy Act, staff must produce a plan that demonstrates why social media is being used and how it will be used. This plan must clearly document what staff intend to do, what they have considered and what training they have undertaken, to adequately defend actions if challenged. Staff should use the appropriate approval template to do this, and ensure that they complete the Social Media Usage Register.

Official Information Act requests for details about social media

Any Official Information (OIA) Act request for details about social media information held about an individual is managed using the usual OIA process.

If the decision is that the request is appropriate to comply with, details will be pulled from the Social Media Usage Register and agreed approach as given in the approval documents.

Care will need to be taken to ensure information about MBIE staff and non-related individuals are redacted from any material provided.

Appendix 1: Template for approval of overt passive membership for an individual or business unit

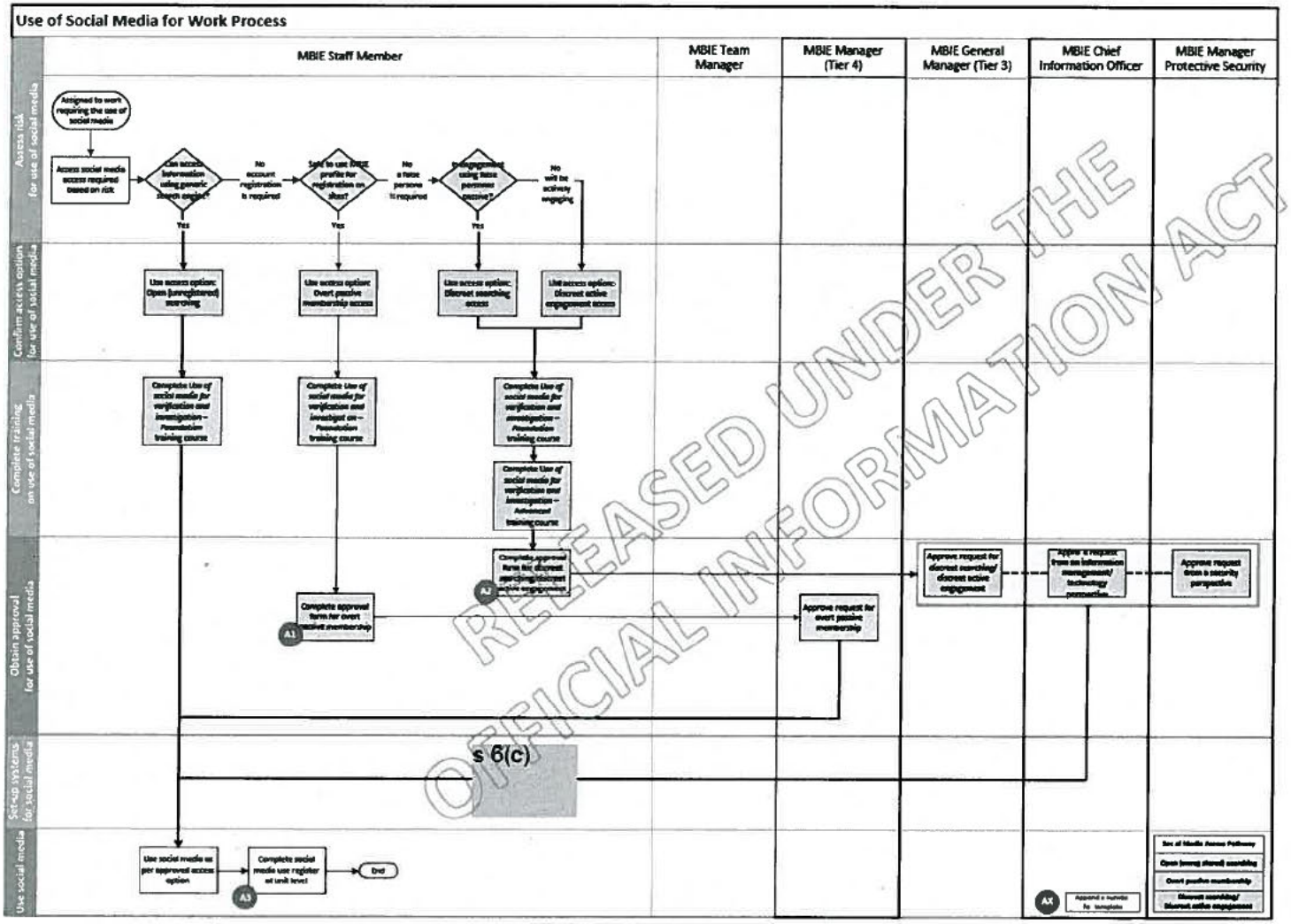
Request to access and use information from social media – OVERT PASSIVE MEMBERSHIP		
Details of staff member requesting to use social media for work purposes		Name, position, unit and group. Include whether the request is at individual or business unit level and whether it is for a one off or ongoing use.
Rationale for accessing and using social media		This section must include the valid and lawful reason for accessing social media – the specifics on what the information is intended to assist with – the purpose.
Plan for collecting information from social media		The plan must describe: • how the staff member will record their social media search activities. • how the staff member will ensure that only information relevant to the purpose is collected. • how information from social media will be verified using other sources. • how the rights of the public in relation to searches by the State are considered and protected.
Where and how the information will be safely and securely stored		For example: Capture a screen shot of the relevant material and then crop or obscure the top and sides of the frame to ensure that the account identity used to gather the information is not revealed. Ensure that the information is named with the access date. Provide directions to where the information will be securely stored, including who has access rights and directions to the unit's Social Media Usage Register.
Competence		Confirmation that all staff members to whom this approval relates have completed the Use of Social Media for Verification and Investigation – Foundation training course.
These three approvals only completed for off-shore requests	**Operations Manager review**	This may be a physical signature or embedded email with agreement to this plan
	Risk Manager assessment	Details the outcome of the risk assessment and whether there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational, or security factors. Risk Manager notes whether local legal advice has been obtained and when it was obtained.
	Area Manager approval	This may be a physical signature or embedded email with agreement to this plan and acceptance of the risk assessment.
Manager (Tier 4 or above) approval		This may be a physical signature or embedded email with agreement to this plan, date of approval and a date for review (usually annual).

Appendix 2: Template for approval of discreet searching or discreet active engagement for an individual or business unit

Request to access and use information from social media – DISCREET SEARCHING & DISCREET ACTIVE ENGAGEMENT		
Details of staff member requesting to use social media for work purposes		Name, position, unit and group. Include whether the request is at individual or business unit level and whether it is for a one off or ongoing use.
Rationale for accessing and using social media		This section must include the valid and lawful reason for accessing social media – the specifics on what the information is intended to assist with – the purpose.
Plan for collecting information from social media		The plan must describe: • what systems and tools will be used to safely access social media • how the staff member will record their social media search activities • how the staff member will ensure that only information relevant to the purpose is collected • how information from social media will be verified using other sources • how the rights of the public in relation to searches by the State are considered and protected • how the false persona will be created and what will happen to the false persona at the end of the investigation.
Where and how the information will be safely and securely stored		For example: Capture a screen shot of the relevant material and then crop or obscure the top and sides of the frame to ensure that the account identity used to gather the information is not revealed. Ensure that the information is named with the access date. Provide a link to where the information will be securely stored, including who has access rights and directions to the unit's Social Media Usage Register.
Competence		Confirmation that all staff members to whom this approval relates have completed both the Use of Social Media for Verification and Investigation – Foundation training course and the Use of Social Media for Verification and Investigation – Advanced training course (or equivalent).
These three approvals only completed for off-shore requests	**Operations Manager review**	This may be a physical signature or embedded email with agreement to this plan.
	Risk Manager assessment	Details the outcome of the risk assessment and whether there are any local factors that pose an additional risk to MBIE. Local factors can include legal, operational or security factors. Risk Manager notes whether local legal advice has been obtained and when it was obtained.
	Area Manager approval	This may be a physical signature or embedded email with agreement to this plan and acceptance of the risk assessment.

General Manager (Tier 3) approval	This may be physical signature or embedded email with agreement to this plan.
Chief Information Officer approval	This may be physical signature or embedded email with agreement to this plan.
Manager Protective Security approval	This may be physical signature or embedded email with agreement to this plan.
Deputy Chief Executive (urgent requests)	For urgent requests, the DCE for the group can approve the request. This may be physical signature or embedded email with agreement to this plan.

Appendix 3: Process Overview



Appendix 4: Social Media Usage Register

Social Media Record of Use

IMPORTANT: Before carrying out any investigative work using social media, ensure you have read he guidance on social media use AND gained he appropriate management approval.

Access Date / Time	Work Branch /Unit	Client Identification Number	Staff Member accessing	Social Media User Name	Social media trigger / Reason for access	Date approved	Type of method used	What was the result of the search?	Was any information captured?	What information was stored?	Where is the material stored?

Decline Register

A register of social media requests that have been declined are to be logged.

Name	Work Branch /Unit	Social media trigger / reason for access		Reason for Decline	Date Declined

Appendix 5: Supporting documents

- Use of Social Media for Verification and Investigation Purposes – Factsheet
- http://s 6(c)
- Use of Social Media for Verification and Investigation Purposes – Approval forms
- http:/ s 6(c)
- Use of Social Media for Verification and Investigation Purposes – Usage Register
- http:/ s 6(c)
- Use of Social Media for Verification and Investigation Purposes – False Persona Guide
- http:/ s 6(c)
- s 6(c)
-
- ICT Acceptable Use Policy:

  ICT Acceptable Use Policy
- Code of Conduct:

  Code of Conduct
- MBIE Social Media Policy:

  Social Media Policy
- MBIE Records Management Policy:

  Records Management Policy
- Privacy Act 1993:

Privacy Act 1993

- **Threat and Intimidation Response Procedure:**

  Threat and Intimidation Response Procedure

- **Staff Personal Security Procedure:**

  Staff Security Procedure